INFORMATION PROTECTION IN VIRTUALIZED ENVIRONMENTS

VERDASYS

Verdasys Digital Guardian is a proven information security platform for Virtual Desktop Interfaces (VDI) and Virtual Machine (VM) environments that can support requirements for extra-network business strategies from remote workforce and partner collaboration, to supply chain integration and global sourcing. Digital Guardian scales to millions of users, and is the only solution capable of enforcing user, data, application, and session-specific policy rules across both physical and virtual machines.

The Virtual Security Challenge: VDI and VM solutions are valued for their cost effectiveness and flexibility, but can create new operational risks because infrastructure-dependent security solutions – like DLP, access control, or network security appliances – are unable to identify, monitor, or enforce policy within virtual environments because the relationships between user, IP address, and machine names on which policy enforcement is based are dissociated.

A data-centric security approach which operates independent of infrastructure is required to protect information within virtual environments. The solution must:

- Enforce policy without network identifiers like machine name or IP address
- Operate across multiple sessions on a single server hosting an array of concurrently-accessed virtual machines
- Enforce policy logic based on the transaction context between user, data, and activity
- Continuously log and reference data events between physical and virtual environments
- Remain a passive monitor until a policy response is needed

Supports user, data, application, *and* session security: Digital Guardian agents operate within a virtual session and on the physical host to provide end-to-end forensic auditing and rules-based policy enforcement – including data classification, encryption, and usage control – from the moment a user logs into their physical machine through VM/VDI creation and termination. Digital Guardian also detects when data is being passed between them to correlate event logs and control local operations like Copy/Move/Save to removable media, Upload, Email, Print, burn to CD/DVD, Copy & Paste, Print Screen, Save As, etc.

Risk-based policy enforcement: Digital Guardian's advanced security sensors operate in both kernel and user-modes simultaneously for precise situational and threat awareness. Agents autonomously confirm potential threats defined by policy – including privileged insiders – and determine the correct enforcement response in real time.

Supports Citrix, VMware, and Microsoft VDI/VM
Infrastructure-agnostic Information Protection
User, Data, Application, and Session-based Policy Enforcement
VDI/VM Insider Threat Mitigation
Remote Access Policy Alerts & Enforcement
Data Control for USB, Print, Save/Save As, Copy & Paste, etc.
Policy-Based and Unified File Encryption
Forensic VM Session Auditing

Digital Guardian's tamper-resistant architecture supports multiple virtual architectures and vendors, including Citrix, VMware, and Microsoft solutions:

Citrix XenDesktop and XenApp

XenDesktop: supported as a hosted VDI, hosted Shared, local VM, or streamed virtual hard drive (VHD)

XenApp: supported as a Shared Desktop and within shared applications

VMware vSphere ESXi, Server, View, Workstation, and ACE

DG agents are embedded within gold images used to dynamically generate VM's

DG agents on the physical host audits and controls user actions and interaction with VM

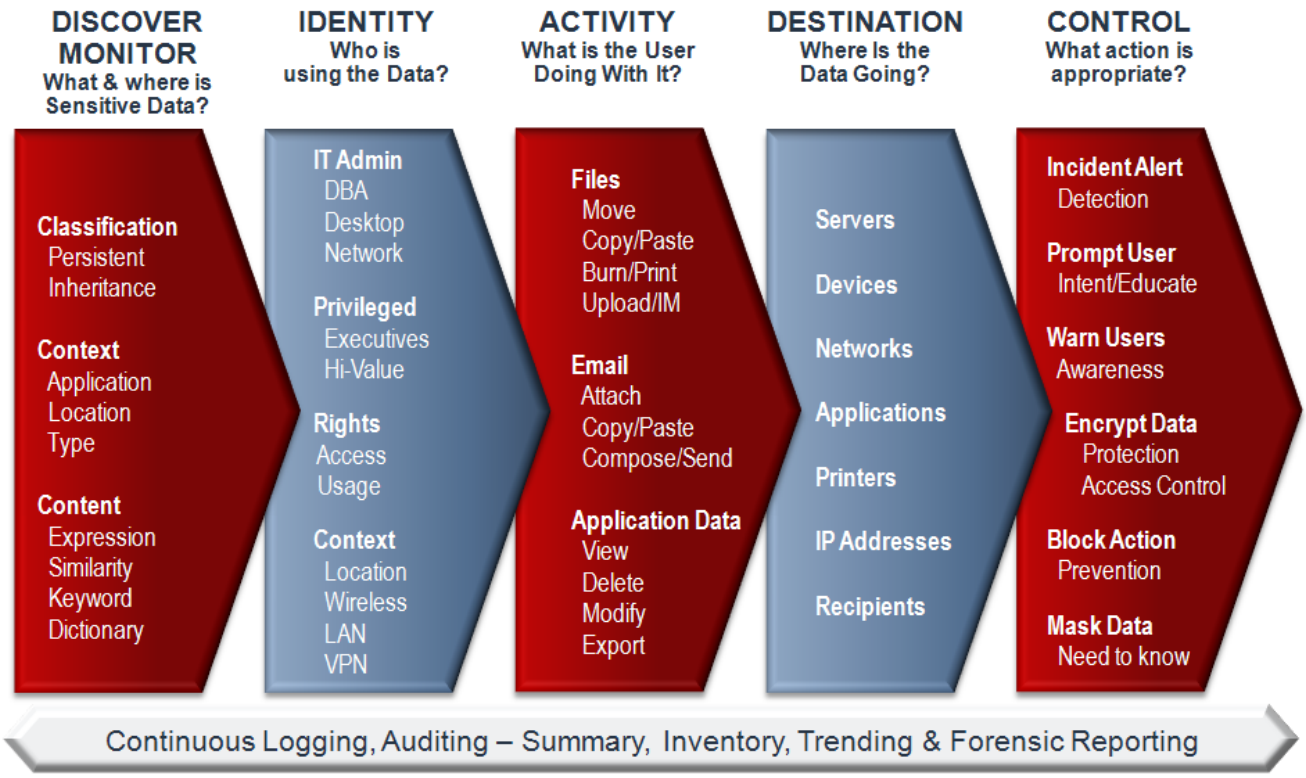
Microsoft Terminal Server and Hyper-V

DG agents supported on Hyper V Server or Server 2008 R2

Corporate Headquarters
404 Wyman Street
Waltham, MA 02451 USA
info@verdasys.com
781-788-8180

WWW.VERDASYS.COM

VDI/VM INFORMATION PROTECTION



VIRTUAL ENVIRONMENT INSIGHT & POLICY ENFORCEMENT:

- Integrated "reference monitor"-based platform for insider threat monitoring, detection, deterrence, and prevention in virtual environments
- Provides continuous capture of system activity as sequenced, compressed, hashed, signed, and encrypted log events
- Proven to scale beyond 500,000 agents reporting continuously to a single backend server
- Multi-tier management architecture supports role-based policy administration and reporting
- Low network utilization; agents report to the management server via secure messaging from anywhere in the world
- Configurable stealth and tamper-resistant agent sources own forensic data at user, data, application, and session levels simultaneously
- Monitors, audits, and controls data transactions between virtual and physical environments
- Monitors, audits, and controls local file operations including to removable media, network upload, email, print, burn to CD/DVD, Copy & Paste, Print Screen, Save, and Save As.
- Policy and reporting architecture supports high availability (HA) and disaster recovery (DR) models
- Integrated, on-board AES 256-bit encryption for transparent or password-based file transfers; includes automated key management and recovery
- Archived log data can be replayed for forensic, investigative or evidentiary purposes

The clear leader in insider threat solutions: Verdasys has been successfully delivering innovative enterprise-class software in the insider threat market for over seven years to the world's largest and most security-conscious organizations. Our unique product and service offerings combined with our execution success at the world's leading companies make Verdasys the de facto leader in the Enterprise Information Protection (EIP) market space.

Support: Verdasys Digital Guardian software runs on Windows 2000, XP, Vista, Windows 7 (32 and 64 bit); Windows 2000 Server, Server 2003, Server 2008; Citrix XenDesktop and XenApp; VMware vSphere ESXi, Server, View, Workstation, and ACE; and Microsoft Terminal Server, and Hyper-V virtual environments

Founded in 2003, Verdasys provides insider threat solutions that are the cornerstone of our customer's global data security strategy. With more than 2 million security agents deployed at over 200 of the world's leading organizations and Federal agencies, our solutions and services provide a strategic and comprehensive approach to information risk management.

Corporate Headquarters
404 Wyman Street
Waltham, MA 02451 USA
info@verdasys.com
781-788-8180

WWW.VERDASYS.COM